REMARKS

Reconsideration of the application in view of the above amendments and the following remarks is respectfully requested. Claims 1, 3, 5, 10, 19, 26, 28, 29, 32, and 33 have been amended. No claims have been canceled or added. Claims 1 - 34 are currently pending in the application.

SUMMARY OF REJECTIONS/OBJECTIONS

Claims 6, 15, 13, 23, and 33 are rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 2, 10, 19, 26, 27, 29, and 32 are rejected under 35 USC 102(e) as being unpatentable by U.S. Publication No. 2002/0016824, published on Feb. 7, 2002, herein *Leeds*. These rejections are traversed.

Claims 4, 5, 8, 9, 11, 15, 16, 17, 18, and 31 are rejected under 35 *USC* 103(a) as being obvious over *Leeds*. These rejections are traversed.

Claims 3, 6, 7, 28, and 30 are rejected under 35 USC 103(a) as being unpatentable over *Leeds* in view of U.S. Patent No. 6,161,130, herein *Horvitz*. These rejections are traversed.

Claims 12, 13, 14 and 20 are rejected under 35 *USC* 103(a) as being unpatentable over *Leeds* in view of U.S. Publication No. 2002/0016916, herein *Natarajan*. These rejections are traversed.

Claims 21 – 25, 33 and 34 are rejected under 35 *USC* 103(a) as being unpatentable over U.S. Publication No. 2002/0026634, herein *Shaw*. These rejections are traversed.

REJECTIONS BASED ON 35 USC 112

Claims 6 and 15 are rejected under 35 USC 112, second paragraph, allegedly because the term "signature elements" is not clearly defined in the specification. Applicant respectfully disagrees. The application contains the following section describing signature elements.

> Signature generator 120 generates message signature 260, which may include one or more signature elements 270. In one embodiment of the present invention, signature generator 120 generates one or more signature elements 270 by applying a one way hash function to a portion of electronic mail message 210. For example, signature generator 120 may read data from a portion of body part 232, and apply a first one-way hash function to the read data to produce element 272. Likewise, signature generator 120 may read data from a portion of body part 234, and apply a second hash function to produce element 274.
>
> Alternatively, signature generator 120 may read portions of multiple body parts within electronic mail message 210, apply a hash value function to the read data to generate element 272. Likewise, signature generator 120 may read other portions of multiple body parts within electronic mail message 210, and apply a hash function to the read data to generate element 274.
>
> There are numerous other mechanisms or techniques that may be used to generate a message signature. For example, a signature element may be generated from a single paragraph, from a single paragraph of a given size, from a set of words in an electronic mail message that are in a dictionary, or from words appearing a given number times, or from all of an electronic mail message but the first and last n lines. Instead of applying a one-way hash function, an signature element may be generated by applying a function that returns a CRC-32 value. Furthermore, it is not necessary that a message signature be a composite data structure with multiple elements or data structures. It may simply be, for example, a single numeric value. Therefore, it is understood that the present invention is not limited to any particular mechanism, technique, or data structure for generating message signatures. (page 15 – page 16)

The above cited section and FIG. 2 of the specification clearly describe that a signature element is a distinct part of a message signature, which may be generated from a portion of an

electronic mail message. In fact, the section describes specific examples. Based on the foregoing, it is respectfully requested that the examiner reconsider claims 6 and 15 and remove the rejection.

Claim 13 is rejected under 35 *USC* 112, second paragraph, because "Routines" is not clearly defined in the specification. Claims 23 and 33 are rejected under 35 *USC* 112, second paragraph, because the term "first set of routines" is too broad and not clearly defined in the specification. The term "routines" as an accepted meaning in the art. In fact, even www.dictionary.com provides a definition, which is "A set of programming instructions designed to perform a specific limited task". Applicant does not intend, nor has applicant indicated in the specification, a meaning that is contrary to that accepted in the art. Finally, the broadness of a claim term is not a proper subject of 35 *USC* 112, second paragraph, (see MPEP 2173.04). Reconsideration of claims 13, 23, and 33 and removal of the rejections is respectfully requested.

REJECTIONS BASED ON PRIOR ART

Claim 1 and 26, as amended, recite:

automatically generating a set of criteria based on contents of a plurality of electronic mail messages received over a network;

wherein the step of automatically generating a set of criteria includes, in response to determining that a threshold number of said plurality of electronic mail messages have a particular content, generating criteria that classifies electronic mail messages that have said particular content as a first type of electronic mail;

Claims 1 and 26 are rejected as being anticipated under 35 USC 102 by *Leeds*. However, claims 1 and 26, as amended, recite features not disclosed or suggested in any way by the cited art, including *Leeds* as well as other art cited as a basis for rejecting other claims. For example, the cited art does not disclose or suggest in any way generating criteria that "classifies electronic

#1

mail messages that have said particular content" in response to "determining that a threshold number of said plurality of electronic mail messages have [the] particular content".

Applicant admits that *Leeds* describes a system that uses criteria to determine that an electronic mail message is junk email. Among the examples of criteria used are the source or transmission path of an electronic mail message (col. 0024, 0032), or inclusion of certain phrases and keywords in the message body (0026, 0034). However, neither of these examples, nor anything else in *Leeds*, suggest in any way using or generating criteria based on a threshold number of electronic mail messages sharing a particular content.

Applicant notes that in rejecting other claims, the Examiner relies on a flawed premise to show obviousness under 35 USC 103. Because the Examiner may be tempted to apply that flawed premise to claims 1 and 26, Applicant is addressing it here.

The flawed premise relied upon is that teaching a particular way of serving a particular function inherently suggests any other way of serving that function. (See for example, section 4, support for rejecting claim 4). This is not incorrect. A particular way of serving a function does not necessarily by itself suggest every possible other way of serving that function. For example, the fact that finger printing and DNA testing serve the function of identifying people does not mean that finger printing suggests in any way DNA testing. Furthermore, the fact that a reference discloses a particular way of serving a function teaches away from serving that function some other way because by teaching that the function is performed in the particular way, the art eliminates the need to find another way to fulfill that function.

Thus, if the Examiner concludes that the teaching of *Leeds* and the step of automatically "generating a set of criteria", as recited in claims 1 and 26, serve the same function of identifying electronic mail messages as junk mail or some other type of mail, this conclusion by itself fails to prove that *Leeds* suggests in any way the particular way of generating a set of criteria claimed,

which includes generating criteria that "classifies electronic mail messages that have said particular content" if "determining that a threshold number of said plurality of electronic mail messages have [the] particular content".

Applicant notes that claim 3 was rejected as obvious in view of *Horvitz* as well as *Leeds*. Because claim 3, before amendment, recited "determining whether at least a portion of the contents in said electronic mail message matches at least a portion of contents of at least a threshold number of said plurality of electronic mail messages", the Examiner may be tempted to apply the reasoning used to reject former claim 3 to claims 1 and 26. In rejecting claim 3, the Examiner admits with respect to claim 3 that *Leeds* fails to "explicitly teach the use of matching a threshold number of electronic mail messages to a portion of the contents in the electronic mail message." (section 5) The Examiner, however, bases the rejection of former claim 3 by alleging that *Horvitz* renders claim 3 obvious by teaching to use a "threshold value to be compared against for filtering out unwanted emails." (section 5, citing *Horvitz*, col. 5, line 67 – col. 5, line 15). Despite teaching this, *Horvitz* nevertheless fails to suggest in any way "determining that a threshold number of said plurality of electronic mail messages have a particular content". In *Horvitz*, the threshold value and the values to which the threshold value is compared, reflect a variety characteristics and criteria about email, as shown below.

> In accordance with our specific inventive teachings, each incoming e-mail message, in such a stream, is first analyzed to determine which feature(s) in a set of N predefined features, i.e., distinctions, (where N is an integer), that are particularly characteristic of spam, the message contains. These features (i.e., the "feature set") include both simple-word-based features and handcrafted features. A feature vector, with one element for each feature in the set, is produced for each such message. The contents of the vector are applied as input to a probabilistic classifier, such a modified Support Vector Machine (SVM) classifier, which, based on the features that are present or absent from the message, generates a continuous probabilistic measure as to whether that message is spam or not. This measure is then compared against a preset threshold value. If, for any

message, its associated probabilistic measure equals or exceeds the threshold, then this message is classified as spam and, e.g., stored in a spam folder. Conversely, if the probabilistic measure for this message is less than the threshold, then the message is classified as legitimate and hence, e.g., stored in a legitimate mail folder. (col. 4, line 54 - col. 5, line 7)

Horvitz, in teaching to compare a threshold value to values that reflect a variety of characteristics or criteria about electronic mail messages, fails to suggest that those values reflect criteria that is based in anyway upon a number of electronic mail messages having been determined to have a particular content, as is required by claims 1 and 26. In fact, the Examiner stops well short of alleging that the values reflect criteria that is based in anyway upon a number of electronic mail messages having been determined to have a particular content, by only alleging that *Horvitz* teaches a threshold value to be compared ...for the reason to classify according to "some criteria" and not alleging that *Horvitz* suggests that the "some criteria" is based in any way on a threshold number of electronic mail messages having a particular content.

For reasons given above, it is respectfully submitted that claims 1 and 26 are not disclosed or suggested in any way by the cited art. Reconsideration of claims 1 and 26 is respectfully requested.

CLAIMS 10 AND 29

Claims 10 and 29, as amended, recite:

an electronic mail server determining whether said message signature satisfies a set of criteria based on message signatures previously received by said central server from a set of electronic mail servers; and

wherein said set of criteria classifies said electronic mail message and a threshold number of electronic mail messages as having a particular content;...

Claims 10 and 29 are rejected as being anticipated under 35 USC 102 by *Leeds*. The cited art fails to disclose or suggest in any way all the limitations of claims 10 and 29. For example, the cited art fails to disclose or suggest in any way the limitation of a "set of criteria [that] classifies said electronic mail message and a threshold number of electronic mail messages as having a particular content", for reasons similar to those discussed with respect to claims 1 and 26. Therefore, claims 10 and 29 are patentable. Reconsideration and allowance of claims 10 and 29 is respectfully requested.

CLAIMS 19 AND 32

Claims 19 and 32 recite:

> determining whether said message signature satisfies a set of criteria that indicates said electronic mail message and a threshold number of electronic mail messages have a particular content;...

Claims 19 and 32 are rejected as being anticipated under 35 USC 102 by *Leeds*. The cited art fails to disclose or suggest in any way all the limitations of claims 19 and 32. For example, the cited art fails to disclose or suggest in any way the limitation of "determining whether said message signature satisfies a set of criteria that indicates said electronic mail message and a threshold number of electronic mail messages have a particular content", for reasons similar to those discussed with respect to claims 1 and 26. Therefore, claims 19 and 32 are patentable. Reconsideration and allowance of claims 19 and 32 is respectfully requested.

CLAIMS 15 AND 31

Claims 15 and 31, recite:

> counts of how many times said one or more signature elements are matched by signature elements from message signatures generated for other electronic mail messages.

Claims 15 and 31 were rejected as being obvious under 35 USC 103 over *Leeds*. The cited art, however, fails to disclose or suggest in any way all the limitations of claims 15 and 31. For example, the cited art fails to disclose or suggest in any way the limitation of "counts of how many times said one or more signature elements are matched by signature elements from message signatures generated for other electronic mail messages", for reasons similar to those discussed with respect to claims 1 and 26. Therefore, claims 15 and 31 are patentable. Reconsideration and allowance of claims 15 and 31 is respectfully requested.

#6

DEPENDANT CLAIMS

The pending claims not discussed so far are dependant claims that depend on an independent claim that is discussed above. Because each of the dependant claims include the limitations of claims upon which they depend, the dependant claims are patentable for at least those reasons the claims upon which the dependant claims depend are patentable. Removal of the rejections with respect to the dependant claims and allowance of the dependant claims is respectfully requested.

In addition, the dependent claims introduce additional limitations that independently render them patentable.

For example, claim 5, recites:

> generating message signatures for each electronic mail message of said plurality of electronic mail messages, wherein each message signature includes one or more message signature elements; and
>
> counting how many of said one or more signature elements match signature elements from other message signatures.

Claim 5 is rejected as being obvious under 35 USC 103 over *Leeds*. However, claim 5 recites limitations not disclosed by *Leeds*. In fact, the Examiner admits that *Leeds* "fails to

explicitly teach tracking how many signature elements of electronic mail messages match." (Section 4, 1st – 3rd paragraph)

The Examiner supports the rejection by alleging that the "confidence rating feature [in *Leeds*] serves the same function as the signature elements tracker because this tracking of signature elements is used to calculate how 'confident' the system is in determining whether the electronic mail is a junk electronic mail." Therefore, the confidence rating feature suggests this feature of claim 5. Even if the allegation were true, which it is not, the fact that a reference teaches a particular way of serving a function does not by itself suggest another way of serving that function. In fact, as mentioned before, such a teaching teaches against another way of serving that function.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: September 13, 2002

Marcel K. Bingham
Reg. No. 42,327

1600 Willow Street
San Jose, CA 95125
Telephone No.: (408) 414-1080 ext.206
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Box Non-Fee Amendment, Commissioner for Patents, Washington, DC 20231.

on September 13, 2002 (Date) by (Signature)

Marked-Up Version of Amendments

Please replace the paragraph starting as page 6, line 10, with the following:

Techniques for identifying which electronic mail messages are "bulk" electronic mail messages are described herein. Rather [then] than rely exclusively on the originators specified in electronic mail messages to determine they are bulk, the techniques make the "bulk determination" based on the contents of the electronic mail messages. Specifically, a set of criteria is automatically generated based on the contents of electronic mail messages. Those electronic mail messages that satisfy the criteria are handled as bulk mail.

Please replace the paragraph starting as page 8, line 6, with the following:

When a central server receives a message signature, the central server generates a count of how many times a matching signature elements in the message signature have been previously received. The central server transmits the count of the most frequently matched signature element to the electronic mail server that transmitted the just received message signature. If the count meets [an] a predetermined threshold, the electronic mail server marks the electronic mail message as bulk electronic mail.

1. (Amended) A method of managing electronic mail, the method comprising the steps of:

automatically generating a set of criteria based on contents of a plurality of electronic mail messages received over a network;

wherein the step of automatically generating a set of criteria includes, in response to determining that a threshold number of said plurality of electronic mail messages have a particular content, generating criteria that classifies electronic mail messages that have said particular content as a first type of electronic mail;[3]

receiving an electronic mail message over said network;

determining whether said electronic mail message satisfies said set of criteria;

if said electronic mail message satisfies said set of criteria, then processing said electronic mail message as ~~a~~[4] said[5] first type of electronic mail; and

if said electronic mail message does not satisfy said set of criteria, then processing said electronic mail message as a second type of electronic mail;

wherein said first type of electronic mail is processed differently than said second type of electronic mail.

2. (Not Amended) The method of Claim 1 wherein:

the method further comprises the step of generating a message signature for said electronic mail message based on contents of said electronic mail message; and

the step of determining whether said electronic mail message satisfies said set of criteria includes determining whether said message signature satisfies said set of criteria.

3. (Amended) The method of Claim ~~1~~[6] 1,[7] wherein ~~the step of~~ [8]determining ~~whether said electronic mail message satisfies said set of criteria includes determining whether at least a portion of the contents in said electronic mail message matches at least a portion of contents of at least~~[9] that[10] a threshold number of said plurality of electronic mail messages have a particular content includes determining that at least a portion of each of said plurality of electronic mail messages have said particular content[11].

4. (Not Amended) The method of Claim 1 wherein the step of generating a set of criteria based on contents of a plurality of electronic mail messages received over said network includes tracking how many signature elements of said electronic mail messages match.

5. (Amended) The method of Claim 1 wherein the step of generating a set of criteria based on contents of a plurality of electronic mail messages received over said network includes the steps of:

generating message signatures for each electronic mail message of said plurality of electronic mail messages, wherein each message signature includes one or more ~~message~~[12] signature elements; and

counting how many of said one or more signature elements match signature elements from other message signatures.

6. (Not Amended) The method of Claim 5 wherein the step of determining whether said electronic mail message satisfies said set of criteria includes determining whether a message signature generated for said electronic mail message includes at least one signature element that matches a threshold number of signature elements of previously generated message signatures.

7. (Not Amended) The method of Claim 6 wherein the step of determining whether a message signature generated for said electronic mail message includes at least one signature element that matches a threshold number of signature elements, further includes determining whether a message signature generated for said electronic mail message includes at least one signature element that matches a threshold number of signature elements of previously generated message signatures that are associated with a period of time.

8. (Not Amended) The method of Claim 1 wherein the step of processing said electronic mail message as a first type of electronic mail includes adding a bulk electronic mail flag to said electronic mail message.

9. (Not Amended) The method of Claim 8, further including the steps of:
after processing said electronic mail message as a first type of electronic mail,
transmitting said electronic mail message to an electronic mail server;
said electronic mail server receiving said electronic mail message;
said electronic mail server determining whether said electronic mail message contains said bulk electronic mail flag; and
if said electronic mail message contains said bulk electronic mail flag, then processing said electronic mail message without further verifying whether said electronic mail message is bulk electronic mail.

10. (Amended) A method of managing electronic mail, the method comprising the steps of:
a central server receiving from an electronic mail server a message signature generated from an electronic mail message;
an electronic mail server determining whether said message signature satisfies a set of criteria based on message signatures previously received by said central server from a set of electronic mail servers; ~~and~~[13]
wherein said set of criteria classifies said electronic mail message and a threshold number of electronic mail messages as having a particular content;[14]
if said received data satisfies a set of criteria, then said electronic mail server processing said electronic mail message as a bulk electronic mail message.

11. (Not Amended) The method of Claim 10, wherein the step of said electronic mail server determining whether said message signature satisfies a set of criteria includes determining whether a portion of said message signature matches a portion of each of a threshold number of message signatures previously received by said central server from said set of electronic mail servers.

12. (Not Amended) The method of Claim 11, wherein:

the step of a central server receiving from an electronic mail server a message signature includes receiving a set of one or more values generated by a one-way hash function; and

the step of said electronic mail server determining whether a portion of said message signature matches includes determining whether at least one of said set of one or more values matches a threshold number of previously received values generated by a one-way hash function.

13. (Not Amended) The method of Claim 12, the method further including the step of transmitting one or more messages to said electronic mail server specifying changes to one or more routines invoked by said electronic mail server to generate message signatures.

14. (Not Amended) The method of Claim 13, wherein the step of transmitting one or more messages includes transmitting platform-independent byte code.

15. (Not Amended) A method of managing electronic mail transmitted over a network, the method comprising the steps of:

a central server receiving from a set of electronic mail servers message signatures generated from electronic mail messages received by said set of electronic mail servers, wherein each message signature includes one or more signature elements;

said central server generating counts of how many times said one or more signature elements are matched by signature elements from message signatures generated for other electronic mail messages; and

said central server transmitting a message reflecting said counts.

16. (Not Amended) The method of Claim 15, wherein:

the step of a central server receiving includes receiving a particular recipient signature associated with a particular message signature; and

the step of generating counts includes generating counts of how many times said one or more signature elements match signature elements that are:

generated for other electronic mail messages, and

associated with a recipient signature that differs from said particular recipient signature.

17. (Not Amended) The method of Claim 16, wherein the step of transmitting messages reflecting said counts includes transmitting said counts.

18. (Not Amended) The method of Claim 16, wherein the step of transmitting messages reflecting said counts includes transmitting signature elements associated with counts greater than a threshold.

19. (Amended) A method of managing electronic mail, the method comprising the steps of:

receiving an electronic mail message over a network;

generating a message signature for said electronic mail message by applying contents of said electronic mail message to a function that produces said message signature;

determining whether said message signature satisfies a set of criteria that indicates said electronic mail message and a threshold number of electronic mail messages have a particular content[15];

if said message signature satisfies said set of criteria, then processing said electronic mail message as a first type of electronic mail; and

if said message signature does not satisfy said set of criteria, then processing said electronic mail message as a second type of electronic mail.

20. (Not Amended) The method of Claim 19, wherein the step of generating a message signature includes invoking a one-way hash function that receives content from said electronic mail message as input and generates said message signature as output.

21. (Not Amended) The method of Claim 19, wherein the method further includes the step of receiving from a remote server data specifying one or more parameters used by said function for generating said message signature.

22. (Not Amended) The method of Claim 19, wherein:
the method further includes the step of receiving code transported from a remote server; and
the step of generating a message signature includes executing said code.

23. (Not Amended) The method of Claim 19, wherein:
the step of generating a message signature includes invoking a first set of routines that perform said function; and
the method further includes the steps of:
receiving code from a remote server, and
updating said first set of routines based on said code.

24. (Not Amended) The method of Claim 23, wherein the step of receiving code includes receiving platform-independent byte code.

25. (Not Amended) The method of Claim 23, wherein the step of receiving code includes receiving machine executable code.

26. (Amended) A computer-readable medium carrying one or more sequences of one or more instructions for managing electronic mail, wherein the execution of the one or more sequences of the one or more instructions causes the one or more processors to perform the steps of:
automatically generating a set of criteria based on contents of a plurality of electronic mail messages received over a network;

wherein the step of automatically generating a set of criteria includes, in response to determining that a threshold number of said plurality of electronic mail messages have a particular content, generating criteria that classifies electronic mail messages that have said particular content as a first type of electronic mail;[16]

receiving an electronic mail message over said network;

determining whether said electronic mail message satisfies said set of criteria;

if said electronic mail message satisfies said set of criteria, then processing said electronic mail message as ~~a~~[17]said[18] first type of electronic mail; and

if said electronic mail message does not satisfy said set of criteria, then processing said electronic mail message as a second type of electronic mail;

wherein said first type of electronic mail is processed differently than said second type of electronic mail.

27. (Not Amended) The computer-readable medium of Claim 26 wherein:

the computer-readable medium further comprises sequences of instructions for performing the step of generating a message signature for said electronic mail message based on contents of said electronic mail message; and

the step of determining whether said electronic mail message satisfies said set of criteria includes determining whether said message signature satisfies said set of criteria.

28. (Amended) The computer-readable medium of Claim 26 wherein ~~the step of~~ [19]determining ~~whether said electronic mail message satisfies said set of criteria includes determining whether at least a portion of the contents in said electronic mail message matches at least a portion of contents of at least~~[20]that[21] a threshold number of said plurality of electronic mail messages have a particular content includes determining that at least a portion of each of said plurality of electronic mail messages have said particular content[22].

29. (Amended) A computer-readable medium carrying one or more sequences of one or more instructions for managing electronic mail, wherein the execution of the one or more sequences of the one or more instructions causes the one or more processors to perform the steps of:

a central server receiving from an electronic mail server a message signature generated from an electronic mail message;

an electronic mail server determining whether said message signature satisfies a set of criteria based on message signatures previously received by said central server from a set of electronic mail servers; and

wherein said set of criteria classifies said electronic mail message and a threshold number of electronic mail messages as having a particular content;[23]

if said received data satisfies a set of criteria, then said electronic mail server processing said electronic mail message as a bulk electronic mail message.

30. (Not Amended) The computer-readable medium of Claim 29, wherein the step of said electronic mail server determining whether said message signature satisfies a set of criteria includes determining whether a portion of said message signature matches a portion of each of a threshold number of message signatures previously received by said central server from said set of electronic mail servers.

31. (Not Amended) A computer-readable medium carrying one or more sequences of one or more instructions for managing electronic mail, wherein the execution of the one or more sequences of the one or more instructions causes the one or more processors to perform the steps of:

a central server receiving from a set of electronic mail servers message signatures generated from electronic mail messages received by said set of electronic mail servers, wherein each message signature includes one or more signature elements;

said central server generating counts of how many times said one or more signature elements are matched by signature elements from message signatures generated for other electronic mail messages; and

said central server transmitting a message reflecting said counts.

32. (Amended) A computer-readable medium carrying one or more sequences of one or more instructions for managing electronic mail, wherein the execution of the one or more sequences of the one or more instructions causes the one or more processors to perform the steps of:

receiving an electronic mail message over a network;

generating a message signature for said electronic mail message by applying contents of said electronic mail message to a function that produces said message signature;

determining whether said message signature satisfies a set of criteria that indicates said electronic mail message and a threshold number of electronic mail messages have a particular content[24];

if said message signature satisfies said set of criteria, then processing said electronic mail message as a first type of electronic mail; and

if said message signature does not satisfy said set of criteria, then processing said electronic mail message as a second type of electronic mail.

33. (Amended) The computer-readable medium of Claim 32, wherein:

the step of generating a message signature includes invoking a first set of routines that perform said function; and

the computer-readable medium further includes sequences of instructions for ~~performingthe~~[25]performing the[26] steps of:

receiving code from a remote server, and

updating said first set of routines based on said code.

34. (Not Amended) The computer-readable medium of Claim 33, wherein the step of receiving code includes receiving platform-independent byte code.